 https://doi.org/10.34836/pk.2022.315.1

Interoperability of EU information systems – a tool to fight terrorism and serious cross-border crime (Part I)

junior inspector dr Edyta Kot[1]

[1] Central Forensic Laboratory of the Police, edyta.kot@policja.gov.pl

Summary

Terrorism and cross-border crimes are complex and diversified problems. They are one of the most serious threats to the modern world, both nationally and internationally. The Act on the *Police* contains the major tasks of this formation, namely: "To cooperate with foreign police forces and their international organisations, as well as European Union bodies and institutions, on the basis of international agreements and treaties and separate regulations" and "The Police also carry out tasks resulting from the legislation of European Union as well as international agreements and arrangements on the rules and within the scope specified therein". In order to carry out statutory tasks, police officers at home and in the world work on the basis of information which is collected and processed in various types of files, registers, collections or databases. This information is exchanged among authorised authorities at home and in the world. This cooperation is aimed at preventing, detecting and combating the most dangerous crime, in particular, terrorism and organised cross-border crime. The latter became very real when controls at the internal borders of the European Union were abolished, through the creation of the Schengen area. From the beginning of the launch of the Schengen area, it has been realised that security within the area and external border management would require a need to create and implement IT systems whose task would be to support the above-mentioned activities. The abolition of border controls and increased migration flows in Europe are conducive to developing cross-border and terrorist crime. Awareness and experience related to the materialisation of the above-mentioned threats initiated strengthening of cooperation among the individual countries of the globe. Strengthening of cooperation became possible following the creation and launch of large-scale information systems, namely: Schengen Information System (SIS), Eurodac, Visa Information System (VIS), Entry/Exit System (EES) and European criminal records information system - third country nationals (ECRIS-TCN). In this part of the publication, in view of the extensive nature of the issue, only SIS and VIS systems have been described, however, I encourage you to enhance your knowledge about other large-scale systems, i.e. Eurodac, Entry/Exit, ECRIS-TCN and the issue related to their interoperability.

Keywords: Schengen Information System, Visa Information System, terrorism, cross-border crime, eu-LISA

Introduction

Bombings which took place in Spain (2004), London (2005), as well as the growing wave of irregular migration in 2015, resulted in a number of problems related to management of the external borders of the European Union and ensuring security in its territory (Jaroszewska-Choraś, 2016). In response to the above-mentioned problems, the EU Member States started work on improving large-scale information systems storing personal information of third-country nationals attempting to enter the Schengen area, which enable access on the part of the competent authorities of EU Member States to the information collected therein, so as to prevent, detect and investigate serious crime within the framework of the competences assigned [Gajda, 2019]. Currently, there are six main EU systems, five of which process biometric data in the form of dactyloscopic data. They include: Schengen Information System (SIS), Eurodac, Visa Information System (VIS), Entry/Exit System (EES) and European criminal records information system - third country nationals (ECRIS-TCN). In the future, it is planned to extend the searches to include the facial image. The sixth European Travel Information and Authorisation System (ETIAS) does not process biometric data.

The European Agency for the Operational Management of Large-Scale Information Systems in the area of freedom, security and justice (eu-LISA) is responsible for the development and operational management of large-scale information systems. This agency was established by Regulation of the European Parliament and of the Council (EU) No 1077/2011

of 25 October 2011[1]. It started its activity on 1 December 2012. The Agency is an EU authority with legal, administrative and financial autonomy. The legal act establishing the Agency has been replaced by the new Regulation (EU) 2018/1726 of 14 November 2018[2].

Eu-LISA is responsible for the development and operational management of large-scale information systems, which are essential instruments for pursuing the asylum policy, EU border management and migration. These systems include the second generation Schengen Information System - SIS II, the Visa Information System - VIS, Eurodac, Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). The Agency works closely with the Member States, EU institutions and EU agencies operating in the area of justice and home affairs. It ensures the development of large-scale IT systems and therefore provides technical support. It contributes to ensuring that Europeans may travel freely within the European Union without any threat to their safety. It implements new technologies thanks to which EU border management becomes more modern, efficient and secure.

Schengen Information System - SIS

Police cooperation occupies a key place in the European Union's policy. Its strengthening in the EU took place in the 80s of the 20th century, and the then main objective was to maintain internal security in the area of the European Communities [Banach-Gutierrez, 2008]. The development of police cooperation within the European Union was initiated by the conclusion, on 14 June 1985, of the Schengen Agreement, called Schengen I, which was signed by five Member States of the European Communities (Belgium, France, Germany, Luxembourg and the Netherlands) in the Luxembourg town of Schengen, situated on the border of Luxembourg, Germany and France. Currently, the Agreement brings together 26 countries. By nature, it was a political agreement between the Member States and provided for the gradual abolition of controls at its internal borders. The abolition of border controls necessitated the intensification of cooperation among the EU MS police services, aimed at constantly combating crime, including cross-border organised crime.

The SIS database consists of a central system, called Central System SIS (CS SIS), Uniform National Interface (NI-SIS) and the Communication Infrastructure between CS-SIS and NI-SIS, which ensures the transmission of data over an encrypted virtual network for the needs of the SIS and the exchange of data between SIRENE Bureaus. As the most important tool for the information exchange in Europe, used for ensuring security and effective border management, the SIS must ensure the continuity of operation of the system at central and national levels. The Central System SIS and the communication infrastructure allow users to access data 24 hours a day, 7 days a week. The data entered into the system by one Member State are accessible to the services and authorities of the other countries responsible for border surveillance, visa issuance and public security. During crossing external borders or a standard police check, it is checked using the SIS whether an item concerned (e.g. a car) or a person are listed in the common database. The data collected in the SIS II can be accessed by, for example: the Police, fiscal control authorities, the Border Guard, the Internal Security Agency, the Military Gendarmerie, the Central Anti-Corruption Bureau, the Military Counterintelligence Service, the Military Intelligence Service and others[3].

The personal data entered into the SIS include: names, surnames, birth names, previously used names and surnames, nicknames, date and place of birth, gender, any nationality held, the indication "armed", "dangerous", the basis for the alert and other information. The items in the following categories are also entered into the SIS[4]: motor vehicles, trailers whose curb weight exceeds 750 kg, caravans, industrial equipment, vessels, engines of vessels, containers, aircraft and their engines, IT equipment, blank public documents which have been stolen, misappropriated, lost, issued identity documents (e.g. passports, identity cards, residence documents, travel documents, driving licences) which have been stolen, misappropriated, lost or cancelled, vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or cancelled, others which have a nature of the above-mentioned documents or number plates, but are false, and other items.

For the purpose of the conclusive identification of persons, the SIS allows to process biometric data relating to a person's physical or physiological characteristics and enable the conclusive identification of that person. These are: photographs, facial images, dactyloscopic data and DNA profiles. Dactyloscopic data in the SIS mean "data on fingerprints and palm prints

[1] Regulation of the European Parliament and of the Council (EU) No 1077/2011 of 25 October 2011 *establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice,* (OJ EU L 286 of 01.11.2011).

[2] Regulation of the European Parliament and of the Council (EU) No 2018/1726 of 14 November 2018 *on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011*, (OJ EU L 295 of 21.11.2018).

[3] Act of 24 August 2007 *on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System* (Journal of Laws of 2007, No.165, item 117).

[4] Ibidem.

which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity"[5]. This means that between one and ten plain and rolled fingerprints are entered into the SIS. They can also contain up to two palmprints[6]. Dactyloscopic data and DNA profiles are used in any case to identify or confirm the identity of a person which has been established as a result of an alphanumeric search carried out in SIS. If the identity of a person cannot be established in any way, a biometric search is carried out in the SIS with an Automated Fingerprint Identification System (so-called SIS in AFIS). Dactyloscopic data are entered into the SIS upon request of the judicial authority of the Member State which enters an alert. These alerts concern[7]:

a) persons wanted for the purpose of being arrested and extradited pursuant to the European arrest warrant (EAW) or being arrested and extradited,
b) missing persons or vulnerable persons who must be prevented from travelling in order to ensure their protection or to eliminate a threat to public security or order,
c) children at risk of being kidnapped by a parent, family member or guardian;
d) children who must be prevented from travelling due to the specific and real threat of being taken from the territory of a Member State;
e) children who may become victims of trafficking, forced marriage, female genital mutilation or other forms of gender-based violence;
f) children who may become victims of terrorist offence or take part in the commission of such offences or may be recruited by armed groups.

Also, it is possible to enter the following alerts into the SIS[8]:

a) concerning unknown persons who are wanted,
b) containing only dactyloscopic data which constitute fingerprints or palmprints preserved at the scenes of terrorist offences or other serious criminal crimes,
c) being the subject of preparatory proceedings.

Those data are entered into the SIS only there is a very high probability that they belong to a perpetrator of the given offence or act of terrorism. In particular, this applies to a situation where the dactyloscopic data have been discovered and preserved on a weapon or other item used in committing a crime or have been searched in available national, EU or international databases with negative results.

Access to data entered into the SIS and the right to search such data directly are granted to national judicial authorities, including those responsible for initiating criminal proceedings in cases prosecuted by public accusation, as well as for conducting preparatory proceedings before making an indictment, as part of carrying out their statutory tasks.

The automated fingerprint identification service introduced within the SIS complements the existing Prüm mechanism regarding cross-border online access to designated national databases containing DNA and dactyloscopic data provided for in Council Decisions 2008/615/JHA[9] and 2008/616/JHA[10]. Thanks to searching for dactyloscopic data in the SIS, it is possible to actively search for a perpetrator. If the search of dactyloscopic data results in a match, the Member State carries out a verification with the participation of experts so as to establish whether there is a match between the dactyloscopic data being searched and the data stored in the SIS. This type of identification is to assist in the preparatory proceedings and to lead to the arrest of a suspect.

Each Member State enters only one alert into the SIS II with regard to a given person or item. The second and subsequent alerts regarding a given person or item are stored at national level so that they can be entered from national level once the first alert has been deleted from the system. Before entering an alert into the SIS II, it is necessary to check whether a given person or item is already in the system. In the case of a person, checking the presence of multiple alerts involves an obligatory comparison of the surname, first name, date of birth, gender, dactyloscopic data. The introduction of the possibility to check a person based on the dactyloscopic data into the SIS II has increased

[5] Act of 24 August 2007 *on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System* (Journal of Laws of 2007 No 165 item 117).

[6] Ibidem.

[7] Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU*, (OJ EU L 312 of 7.12.2018).

[8] Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU*, (OJ EU L 312 of 7.12.2018).

[9] Council Decision 2008/615/JHA of 23 June 2008 *on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*, [OJ EU L 210 of 06.08.2008].

[10] Council Decision 2008/616/JHA of 23 June 2008 *on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*, (OJ EU L 210/12 of 06.08.2008).

the probability of identifying existing alerts on the same person using different identities[11]. In the SIS II, "hit" and "match" have different definitions. We can talk about a hit in the SIS II when, as a result of a check, the user receives information about a foreign alert in the system and the data regarding the SIS II alert match the data entered for the purpose of the check. These are alphanumeric data. A match occurs when the user searches for fingerprints from among the data stored in the SIS-AFIS. The user receives a notification from the SIS II about the possibility of matching and then is obliged to carry out a procedure of verification for the conformity of fingerprints. In Poland, the verification is carried out by the Department of Dactyloscopic and Traceological Studies of CFLP, to which fingerprint images are sent for the purpose of comparison[12].

Where dactyloscopic data are not available, a Member State should enter alerts on DNA profile into the SIS II. Those profiles should facilitate the identification of missing persons in need of protection, in particular, missing children, among others, in a situation where the use of DNA profiles of immediate relatives for identification is allowed. DNA data should contain only the minimum information necessary to identify a missing person. DNA profiles should not be processed for any purpose other than that for which they have been entered into the SIS[13].

Upon joining the EU on 1 May 2004, Poland became responsible for securing one of the longest sections of the common external land border in the east of the country. Having regard of the above, in August 2007 the Sejm of the Republic of Poland adopted the Act *on the participation of the Republic of Poland in the Schengen Information System (SIS) and the Visa Information System (VIS)*. This Act defines the rules and procedure for the participation of the Republic of Poland in these systems, including the obligations of the authorities entering alerts and the authorities authorised to access the data through the National Information System.

Council Regulation (EC) No 871/2004 of 29 April 2004 *concerning the introduction of some new functions for the Schengen Information System*[14], extended the group of entities authorised to use the SIS data for the purpose of combating terrorism. This Regulation was amended by Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 *on the establishment, operation and use of the second generation Schengen Information System (SIS II)*[15]. The SIS II functions as a single information system despite the fact that it is based on two legal bases, namely Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 and Council Decision 2007/533/JHA of 12 June 2007[16]. This system has been operating since 9 April 2013 and allows to process more data and to use modern functionalities[17]. The authorities authorised to access and directly search data entered into the SIS II are "national judicial authorities, including those responsible for initiating criminal proceedings in cases prosecuted by public accusation, as well as for conducting preparatory proceedings before making an indictment, as part of carrying out their tasks laid down by the national legislation and by the authorities performing a coordinating function towards them" as well as the authorities responsible for establishing the identity of third-country nationals for the purposes of border control, as well as of police and customs checks[18]. According to the assumptions, an important advantage of the second generation Schengen Information System is the improvement in data quality and the ability to identify persons. Modern information technologies allow to process alphanumeric data and biometric data, such as facial images, DNA or fingerprints, in the SIS II. This results in the more efficient and accurate identification of persons[19]. Fingerprint images are used only for the purpose of confirming the identity of a third-country national who has been found in the SIS II while searching according to alphanumeric data[20].

On 19 November 2018, the Council adopted three regulations, known in brief as "SIS Recast", concerning

[11] Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 *replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II),* (OJ EU L 231 of 07.09.2017).

[12] Ibidem.

[13] Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU*, (OJ EU L 312 of 7.12.2018).

[14] OJ EU L 162 of 30.04.2004

[15] OJ EU L 381 of 28.12.2006

[16] OJ EU L 205 of 7.8.2007

[17] Council Decision of 7 March 2013 *fixing the date of application of Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second-generation Schengen Information System (SIS II)* and Council Decision of 7 March 2013 *fixing the date of application of Decision No 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II),* [OJ EU L 2013.87.8 and OJ EU L 2013. 87.10].

[18] Ibidem, Article 27(1) and (2).

[19] https://www.policja.pl/pol/sirene/sis/12473,Co-to-jest-System-Informacyjny-Schengen-SIS.html.

[20] Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 *on the establishment, operation and use of the second-generation Schengen Information System (SIS II),* Article 22 (OJ EU L 381 of 28.12.2006).

the use of the Schengen Information System, which will gradually replace the currently applicable EU regulation and decision. These are[21]:

a) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 *on the use of the Schengen Information System for the return of illegally staying third-country nationals,*
b) Regulation of the European Parliament and of the Council (EU) 2018/1861 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006,*
c) Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.*

Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 provides the basis for searching biometric data, including dactyloscopic data, for identification and detection purposes. The automated dactyloscopic identification within the SIS complements the Prüm mechanism as mutual cross-border on-line access to relevant national dactyloscopic databases. A novelty is the collection and search in the SIS databases of unidentified fingerprints or palmprints that have been discovered and preserved at the scene of a serious crime or terrorist offence. The Regulation defines them as dactyloscopic data, or "data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity[22]".

Under this regulation, it will also be possible to process DNA profiles to identify missing persons, in particular, missing children[23]. The other two Regulations provide the basis for the processing of dactyloscopic data for identification purposes.

The implementation of EU regulations necessitated a need to adapt the provisions of the current Act of 24 August 2007 *on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System*, which contains the legislation enabling the participation of Poland in the SIS and VIS.

Visa Information System (VIS)

The Visa Information System (VIS) allows the Schengen Member States to exchange visa data. For the purpose of identification of persons and verification of identity, the biometric identification is carried out in the system, mainly on the basis of fingerprints[24].

The VIS was established by Council Decision 2004/512/EC of 8 June 2004 *establishing the Visa Information System (VIS)* as a system for the exchange of visa data among the Member States. In turn Regulation of the European Parliament and of the Council (EC) No 767/2008 of 9 July 2008 *concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas* (known in brief as the VIS Regulation) defines the purpose of the Visa Information System[25].

In Poland, the VIS was launched on 11 October 2011. In accordance with the Act of 24.08.2007 *on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System*, it allows designated individual users and institutions to use the applications „VIS", „www VIS", „VISMail"[26]. The Visa Information System is based on a centralised architecture. It consists of a central information system, called the "Central Visa Information System" (CS-VIS), an interface located in each Member State, called the "national interface" (NI-VIS). A component of the system is also communication infrastructure enabling communication between the Central Visa Information System and the national interfaces[27]. The Central Visa Information System (CS-VIS) receives images of plain ten fingerprints with a resolution of 500 dpi (acceptable deviation ± 5 dpi) in 256 shades of grey[28].

The objective of the Visa Information System is to improve consular cooperation and the exchange of information among the Schengen countries with regard to visas issued and visa applicants. The system improves cooperation among the Member States, among others, with regard to the common visa policy, including the simplification of the visa application procedure, the prevention of visa shopping and the identification of persons who may not meet the conditions for entry, stay or residence in the territory of the European

[21] OJ EU L 312 of 7.12.2018

[22] Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU*, Article 3(13), (OJ EU L 312 of 7.12.2018).

[23] Ibidem, point 26.

[24] https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/.

[25] OJ EU L 218 of 13.08.2008.

[26] Journal of Laws No. 165, item 1170, as amended.

[27] file:///C:/Users/CLKP%20Z3/Downloads/Sprawozdanie_z_dnia_24_10_2013.pdf.

[28] Commission Decision of 9 October 2009 *laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the Visa Information System* (OJ EU L 270 of 15.10 2009).

Union. The use of biometric technology makes it possible to detect persons using other person's travel documents, which protects travellers from identity theft and allows to carry out faster, more accurate and secure checks. The system also facilitates the visa issuance process, which is essential for frequent travellers and also makes it possible to determine which EU country is responsible for examining an application for international protection. In addition, the VIS results in improving security as it helps authorities in preventing, detecting and investigating terrorist offences and other serious crimes.

The VIS records and processes alphanumeric data related to a visa applicant and information on visas with an application submitted, issued, cancelled, revoked, extended and refused visas. In addition to alphanumeric data, the system processes photographs, fingerprints, links to previous visa applications and application files created for persons travelling together. The entry of data into the VIS takes place through the visa authorities. Upon acceptance of an application, the relevant authority creates a data file containing information, e.g. personal data, travel details of a visa applicant from the application form, photographs and fingerprints. Should a decision on issuing a visa be made, the visa authority adds additional important information to the application data file, including the type of visa, the territory in which a visa holder is authorised to travel, the visa validity period, the number of entries into the territory where it is valid and the length of stay. It is also necessary to add supplementary data when a visa authority from another EU country discontinues to examine an application or decides to refuse, cancel or revoke a visa, and also in the case of extending the visa validity period[29].

Visa applicants have 10 fingerprints and a digital photograph taken. These biometric data, along with the data provided in the visa application form, are recorded in a secure central database. Applying for a new visa, for frequent travellers to the Schengen area, does not require taking fingerprints every time. Once recorded in the VIS, fingerprints are available for a period of 5 years and may be used for subsequent visa applications submitted during that time[30].

At the external borders of the Schengen area, fingerprint images of a visa holder are compared with the data contained in the VIS database. Any difference between the dactyloscopic data results in launching a procedure for further checking of a traveller's identity. The authorities responsible for carrying out customs clearances at the external borders and in the territory of the country have access to searching information in the VIS using the number of a visa sticker, including the verification of fingerprints of a visa holder. Those authorities are authorised to search the VIS so as to verify the identity of a person or the authenticity of a visa, as well as to confirm whether a given person meets the conditions necessary for entry, stay or residence in the territory of the country. If the search of information indicates that data on a visa holder are recorded in the VIS, the competent border control authority may review the specific data contained in the visa application file.

In order to identify a person who does not meet or no longer meets the required conditions, the competent authorities have access to searching information by means of fingerprints of a given person. Where the use of a person's fingerprints is not possible or the search is negative, the competent authorities may search the VIS using alphanumeric data such as: surname, gender, date and place of birth and other information contained in the travel document. The above search criteria may be used in combination with the criterion of nationality of a given person.

The authorities responsible for granting international protection have access to search the VIS with dactyloscopic data, but only for the purpose of determining the EU country responsible for examining an international protection application.

Information contained in the VIS is not provided to third countries or international organisations, except where the provision of these data is necessary to confirm the identity of a third-country national. The provision of information may be used only in individual, reasonable cases, without prejudice to the rights of refugees and applicants for international protection[31].

Conclusion

When analysing the issue of strengthening international cooperation based on the exchange of dactyloscopic data, it has been found that: existing European large-scale systems are extended to include new functionalities and a wider range of data processed. This applies to the SIS, VIS which, as the second-generation systems, are enriched with images of palmprints and unidentified fingerprints preserved at the crime scene. These changes entail a need to adapt the national legislation as well as to introduce organisational changes in the area of tasks carried out by the authorities and institutions involved in cooperation. The European Union has developed a multitude of legislative acts being the foundation for creating an effective system for combating terrorism and cross-border crime. The basis of this system is already in place and its development in terms of extending the possibilities of using dactyloscopic data and other biometric data, e.g.

[29] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 *concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas* (OJ EU L 218 of 13.08.2008).

[30] https://poland.tw/web/tajwan/wizy--informacje-ogolne.

[31] https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/.

facial image or DNA, contributes to strengthening international cooperation between law enforcement and judicial authorities. The extension of the scope of data processing increases the possibility of identifying persons or detecting a perpetrator of a crime and imposes new tasks on the Police. The next issue of the „Issues of Forensic Science" will describe other large-scale systems, i.e. Eurodac, Entry/Exit, ECRIS-TCN, and the assumptions for the interoperability of these systems as EU IT tools for external border management and prevention and combating of irregular migration.

Bibliography

1. Banach-Gutierrez, J. (2008). Współpraca policyjna w Unii Europejskiej: od TREVI do Schengen III. W: L. Boguni, (ed.), *Nowa Kodyfikacja Prawa Karnego*: *Tom XXIII.* Uniwersytet Wrocławski.
2. Gajda, A. (2019). Interoperacyjność unijnych systemów informacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami. *Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace"*, *1*(37).
3. Jaroszewska-Choraś, D. (2016). *Biometria. Aspekty prawne*. Wydawnictwo Uniwersytetu Gdańskiego.

Legal acts

1. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ EU L 210 of 06.08.2008.
2. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ EU L 210/12 of 06.08.2008.
3. Commission Decision of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the Visa Information System, OJ EU L 270 of 15.10 2009.
4. Council Decision of 7 March 2013 fixing the date of application of Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision of 7 March 2013 fixing the date of application of Decision No 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ EU L 87/10 of 27.03.2013 and OJ EU L 87/8 of 27.03.2013.
5. Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second-generation Schengen Information System (SIS II), OJ EU L 231 of 07.09.2017.
6. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), Article 22, OJ EU L 381 of 28.12.2006.
7. Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ EU L 218 of 13.08.2008.
8. Regulation of the European Parliament and of the Council (EU) No 1077/2011 of 25 October 2011 *establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice,* OJ EU L 286 of 01.11.2011.
9. Regulation of the European Parliament and of the Council (EU) No 2018/1726 of 14 November 2018 *on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011*, OJ EU L 295 of 21.11.2018.
10. Regulation of the European Parliament and of the Council (EU) 2018/1862 of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU*, OJ OJ L 312 of 7.12.2018.
11. Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, Journal of Laws of 2007, No.165, item 117.

Websites

1. https://www.policja.pl/pol/sirene/sis/12473,-Co-to-jest-System-Informacyjny-Schengen-SIS.html, (accessed on: 20.05.2022).
2. https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/, (accessed on: 07.03.2019).
3. https://poland.tw/web/tajwan/wizy--informacje-ogolne, (accessed on: 28.03.2021).

Translation GTC AMG Sp. z o. o.